REALLOC

Not suitable for use with secure memory because memory contents are not zeroed out

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3399 bytes

Attack Category	• Memory Scanning
Vulnerability Category	• Information Leakage
Software Context	• Memory Management
Location	
Description	realloc() is not suitable for use with secure memory because memory contents are not zeroed out. The realloc() function takes an allocated memory block and expands (or contracts) it to a bigger (or smaller) size. This may involve moving the chunk of memory and copying over the old contents. When this is done, the old contents are discarded and left in memory somewhere. For secure memory applications where it is important to erase all traces of data, this behavior is inappropriate. Realloc() has a variety of other sensitive issues related to reliability. Since it moves memory around, any old pointers to that memory become invalid and could cause the program to crash or otherwise misbehave.
APIs	**Function Name** / **Comments** realloc
Method of Attack	Sensitive data may be left in memory and could potentially be accessed by an attacker.
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy** Sensitive data needs to be in a resized memory block. / Do not use realloc for secure memory. If no secure version of realloc is available, / Effective. Reliability risks still possible; however, if old copies of pointer are left around.

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

		use malloc and a secure version of memset(). See MEMSET rule for appropriate usage.	

Signature Details	void *realloc(void *ptr, size_t size)

Examples of Incorrect Code	`[...]`
	`ptr = realloc(ptr, NEW_SIZE);`
	`[...]`

Examples of Corrected Code	`[...]`
	`char * newptr = malloc(NEW_SIZE);`
	`memset(newptr, 0, NEW_SIZE);`
	`memcpy(newptr, ptr, min(OLD_SIZE, NEW_SIZE));`
	`secureMemset(ptr, 0, OLD_SIZE); /* doesn't get optimized away */`
	`ptr = newptr;`
	`[...]`

Source Reference	• man page for realloc()
Recommended Resource	
Discriminant Set	**Operating Systems**: • Windows • UNIX **Languages**: • C • C++

Cigital, Inc. Copyright

1. mailto:copyright@cigital.com